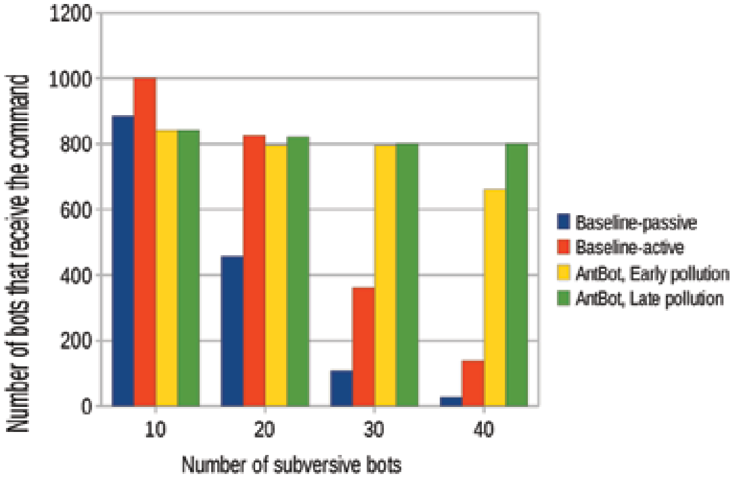
Using the MIITS-Cyber Tool to Analyze Large-scale Cyber Threats

Guanhua Yan, Stephan Eidenbenz, CCS-3

As computer networks have permeated almost every aspect of the nation's critical infrastructure such as its transportation, power grid, communications, and defense, the importance of ensuring a secure and robust information technology (IT) infrastructure is tremendous. The direct costs of cybercrime to the US economy reach tens of billions of dollars annually [1], and the federal government spends billions of dollars on cybersecurity each year [2]. Given the increasing intensity of cyber threats, the Obama administration has recently claimed cyber security a national security priority.

A virtual controllable testbed is an indispensable tool to evaluate the effect of potential cyber threats and the effectiveness of proposed countermeasures. As large-scale cyber attacks (malware, botnet, and distributed denial of service [DDoS] attacks) commonly involve many machines, such an evaluation testbed should not only capture the realism necessary for the analysis, but also have the merit of high scalability. Towards this end, we extended the capabilities of the LANL-developed modeling and simulation suite MultiScale Integrated Information and Telecommunications System (MIITS) and studied two emergent large-scale cyber threats: botnets, which use the peer-to-peer (P2P) networks for their command and control (C&C), and malware, which spread in large cyber social networks (e.g., Twitter and Facebook). The simulation modules that fulfill the analysis of these two cyber threats are called BotSim and CyberSim, respectively.

Fig. 1. Resilience of AntBot against pollution-based mitigation.



BotSim. To achieve great realism in modeling P2P behaviors by P2P-based botnets, we use the actual development code of a popular P2P client, aMule, which is based on the KAD protocol, a variant of Kademlia [3]. It is known that P2P-based botnets, although they do not suffer a single point of failure as IRC-based botnets do, can be effectively disrupted by polluting the command keys [4]. We, however, predict potential moves by the botmaster and find that a new type of hypothetical botnet (dubbed AntBot) works resiliently against pollution-based mitigation [5]. The key idea is to use a tree-like multilevel structure to relay C&C messages from the botmaster in P2P networks. Figure 1 shows the resilience of this hypothetic P2P-based botnet against pollution-based mitigation for a 1000-node botnet. The baseline cases refer to the botnets that do not deploy the antipollution scheme. From the figure, it is clear that even with a number of subversive bots controlled by the white-hat defender, the majority of the bots can still obtain the command issued by the botmaster, regardless of the pollution scheme used by the white-hat defender. The take-home message from this study is that cyber defenders should not be content with their capability of defending against past observed cyber attacks, but should also deploy proactive defense systems that prevent future unobserved cyber attacks from happening.

CyberSim. Virus propagation in social networks has been intensely studied in the literature, especially from a structural perspective. For online social networks, virus propagation is affected by user activities, such as when the user goes online. From a real-world trace, we find that the number of activity events generated by each user in an online social network is well characterized by an extended exponential distribution. The highly skewed distribution of online user activities significantly affects how virus propagates in online social networks. We developed CyberSim, which can be driven by activity traces of real-world online social network users, to quantify

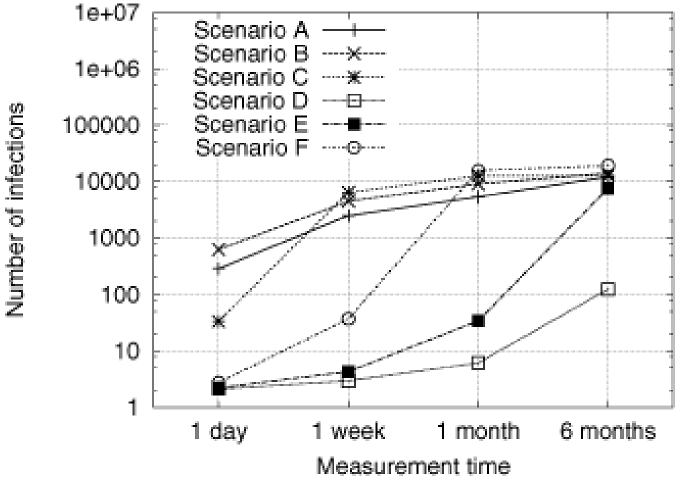


Fig. 2. Virus propagation under different scenarios.

the impact of social structures and user activity patterns on virus propagation [6]. Using CyberSim, we investigate virus propagation under six different scenarios—Scenarios A, B, and C use a real-world social structure, and Scenarios D, E, and F use the Erdos-Renyi social structure; Scenarios A and D use real-world activity events; Scenarios B and E randomize the time intervals among activity events by each user; Scenarios C and F randomize the time intervals among activity events across all the users. Figure 2 depicts the propagation progress by the virus under different scenarios.

From the results, we conclude that the realistic social structure, which has been shown to be a power-law and small-world graph, spreads the virus quickly at its early stage compared with the Erdos-Renyi social structure. Also, we see that the highly skewed distribution of activity events among online users in the real-world dataset actually slows down the virus propagation process. This suggests that future work on analyzing virus propagation in social networks should consider not only realistic social graphs but also realistic human activity models.

For more information contact Guanhua Yan at ghyan@lanl.gov.

[1] 2005 FBI/CSI computer crime survey, http://www.gocsi.com, January (2006).
[2] Pulliam, D. "Cybersecurity spending estimated to grow to $7.1 billion by 2009," *Government Executive,* http://www.govexec.com/dailyfed/0305/031705p1.htm (2005).
[3] D.T. Ha et al., "On the Effectiveness of Structural Detection and Defense agains P2P-based Botnets," *Proc. 39th Ann. IEEE/IFIP Int. Conf. Dependable Systems Networks (DSN'09)* (2009).
[4] T. Holz et al., "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm worm," *Proc. 1st Usenix Workshop Large-Scale Exploits and Emergent Threats (LEET'08)* (2008).
[5] G. Yan, D.T. Ha, S. Eidenbenz, *AntBot: Anti-Pollution Peer-to-Peer Botnets,* LA-UR 09-06004.
[6] G. Yan et al., *Towards A Deep Understanding of Malware Propagation in Online Social Networks,* LA-UR 09-08100.

Funding Acknowledgments
DHS, National Infrastructure Simulation and Analysis Center (NISAC) Program